SOMI Systems a.s. Banská Bystrica

BEZPEČNOSTNÝ PROJEKT

Obec Bacúch

Banská Bystrica, máj 2017

Obec Bacúch vedená snahou o kvalitné a zodpovedné riadenie a zabezpečovanie svojej bezpečnosti vypracovala a prijala tento bezpečnostný projekt. Bezpečnostný projekt sa dňom schválenia vo vedení obce stáva interným prevádzkovým predpisom a je záväzný pre všetkých zamestnancov obce.

Bezpečnostný projekt zodpovedá svojím obsahom, postupmi spracovania a formou nasledovným predpisom a normám:

1. Zákon 122/2013 Z. z. o ochrane osobných údajov v platnom znení.
2. Vyhláška Úradu na ochranu osobných údajov č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení v platnom znení.
3. STN ISO/ETC 27001.
4. STN ISO/ETC 27002.
5. STN ISO/ETC 27005.

Bezpečnostný projekt v súlade s ustanovením § 5 ods. 4 vyhlášky č. 164/2013 Z. z. v platnom znení sa týka nasledovných informačných systémov:

- IS Agenda školstva
- IS Aktivačná činnosť
- IS Dobrovoľná požiarna ochrana
- IS Dochádzka
- IS Elektronická schránka
- IS ePodateľňa
- IS Evidencia o pohrebníctve
- IS Hlavného kontrolóra
- IS Hospodárska mobilizácia
- IS Integrované obslužné miesto
- IS Kamerový systém
- IS Knižnica
- IS Komisií obecného zastupiteľstva
- IS Majetok
- IS Materskej školy
- IS Matričný úrad
- IS Miestne dane a poplatky
- IS Notifikácie a sťažnosti
- IS Obecné zastupiteľstvo a komisia
- IS Ochrana osobných údajov
- IS Overovanie listín a podpisov
- IS Oznamovanie protispoločenskej činnosti
- IS Personalistika a mzdy
- IS Podujatia
- IS Pokladňa
- IS Posudky
- IS Priestupkové konania

- IS Register obyvateľov
- IS Rybárske lístky
- IS Samostatne hospodáriaci roľník
- IS Sociálnych vecí
- IS Správa registratúry
- IS Starostu obce
- IS Stavebný úrad a územné plánovanie
- IS Školská jedáleň
- IS Trhovisko
- IS Účtovníctvo
- IS Verejné obstarávanie
- IS Výrub stromov
- IS Zmluvy
- IS Žiadosti podľa infozákona
- IS Životné prostredie

Bezpečnostný projekt je tvorený nasledovnými dokumentmi, ktoré tvoria jeho neoddeliteľné a navzájom súvisiace súčasti:

1. Bezpečnostný zámer,
2. Analýza rizík I, II,
3. Návrhy opatrení,
4. Bezpečnostná smernica.

Schválil dňa:

_____
Starosta obce

Obsah

1. Úvod

Ochrana osobných údajov, citlivých údajov, majetku a iných aktív je prirodzenou snahou každej organizácie. Problematiku ochrany osobných údajov rieši zákon NR SR č. 122 z roku 2013 v znení neskorších predpisov. Kľúčovým dokumentom, ktorý musí väčšina organizácií spracovať na úseku ochrany osobných údajov, je bezpečnostný projekt, ktorý je v súlade s vyššie spomenutým zákonom definovaný nasledovne:

1. Bezpečnostný projekt vymedzuje rozsah a spôsob technických, organizačných a personálnych opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.
2. Bezpečnostný projekt sa spracúva v súlade so základnými pravidlami bezpečnosti informačného systému vydanými bezpečnostnými štandardmi, právnymi predpismi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná.
3. Bezpečnostný projekt obsahuje:
   - bezpečnostný zámer,
   - analýzu bezpečnosti informačného systému,
   - bezpečnostné smernice.
4. Bezpečnostný zámer vymedzuje základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu informačného systému pred ohrozením jeho bezpečnosti a obsahuje najmä:
   - formuláciu základných bezpečnostných cieľov a minimálne požadovaných bezpečnostných opatrení,
   - špecifikáciu technických, organizačných a personálnych opatrení na zabezpečenie ochrany osobných údajov v informačnom systéme a spôsob ich využitia,
   - vymedzenie okolia informačného systému a jeho vzťah k možnému narušeniu bezpečnosti,
   - vymedzenie hraníc určujúcich množinu zvyškových rizík.
5. Analýza bezpečnosti informačného systému je podrobný rozbor stavu bezpečnosti informačného systému, ktorá obsahuje najmä:
   - kvalitatívnu analýzu rizík, v rámci ktorej sa identifikujú hrozby pôsobiace na jednotlivé aktíva informačného systému spôsobilé narušiť jeho bezpečnosť alebo funkčnosť; výsledkom kvalitatívnej analýzy rizík je zoznam hrozieb, ktoré môžu ohroziť dôvernosť, integritu a dostupnosť spracúvaných osobných údajov, s uvedením rozsahu možného rizika, návrhov opatrení, ktoré eliminujú alebo minimalizujú vplyv rizík, a s vymedzením súpisu nepokrytých rizík,
   - použitie bezpečnostných štandardov a určenie iných metód a prostriedkov ochrany osobných údajov; súčasťou analýzy bezpečnosti informačného systému je posúdenie zhody navrhnutých bezpečnostných opatrení s použitými bezpečnostnými štandardmi, metódami a prostriedkami.
6. Bezpečnostné smernice upresňujú a aplikujú závery vyplývajúce z bezpečnostného projektu na konkrétne podmienky prevádzkovaného informačného systému a obsahujú najmä:
   - popis technických, organizačných a personálnych opatrení vymedzených v bezpečnostnom projekte a ich využitie v konkrétnych podmienkach,
   - rozsah oprávnení a popis povolených činností jednotlivých oprávnených osôb, spôsob ich identifikácie a autentizácie pri prístupe k informačnému systému,
   - rozsah zodpovednosti oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov,

- spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému,
- postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou.

Tento dokument v ďalšom obsahuje bezpečnostný zámer, analýzu rizík a návrh smerníc a opatrení, ktoré autor odporúča prijať s cieľom zvýšiť bezpečnosť osobných údajov a organizácie ako celku. Aj keď pri vypracovaní tohto projektu bol položený dôraz najmä na ochranu osobných údajov, v rizikovej analýze boli posudzované aj hrozby a riziká v širších súvislostiach. Dôvodom tohto prístupu je fakt, že bezpečnosť informačného systému alebo bezpečnosť osobných údajov sa nedá riešiť oddelene od iných problémov, najmä objektovej a personálnej bezpečnosti. Tento dokument nerieši problematiku ochrany utajovaných skutočností (v súlade so zákonom 215/2004 Z. z. o ochrane utajovaných skutočností v platnom znení).

2. Bezpečnostný zámer

2.1. Strategické ciele bezpečnosti

Obec Bacúch deklaruje na účely vypracovania tohto bezpečnostného projektu nasledovné strategické ciele bezpečnosti:

- Vybudovať a trvalo udržiavať vysokú úroveň ochrany a bezpečnosti informačného systému.
- Vytvoriť podmienky a realizovať bezpečné rozmiestnenie najdôležitejších komponentov a trvalo zabezpečovať ich technickú a režimovú ochranu.
- Obstarávať a implementovať informačné systémy len vysokej kvalitatívnej a odbornej úrovne a úžitkovej hodnoty, ktoré budú vytvárať a ochraňovať dobré meno obce Bacúch.
- Uplatniť pri budovaní bezpečnostného systému princíp vlastníctva.
- Chrániť práva zamestnancov, občanov a dodávateľov obce Bacúch.
- Zabezpečiť potrebnú ochranu majetku obce Bacúch.
- Zabezpečiť ochranu finančných prostriedkov.
- Zabezpečiť adekvátnu ochranu zamestnancov pracujúcich s finančnými prostriedkami.
- Zaviesť systém kontrol výkonu práce všetkých oddelení a samotných zamestnancov s cieľom odhaliť nekvalitný, neprofesionálny alebo inak so záujmami obce Bacúch nezlučiteľný výkon práce.
- Zabrániť existujúcim formám obohacovania sa na úkor obce Bacúch.
- Vytvoriť a udržiavať havarijné plány pre všetky dôležité funkcie obce Bacúch.
- Zaviesť a trvalo zabezpečovať systém hlásení o stave bezpečnostného systému a hlásení o bezpečnostných incidentoch.

2.2. Bezpečnostné ciele, zásady ochrany aktív

Obecný úrad v Bacúchu je výkonným orgánom obecného zastupiteľstva a starostu obce, pričom zabezpečuje ich organizačné a administratívne záležitosti. Hlavný cieľom Obecného úradu v Bacúchu je úspešne poskytovať služby obyvateľstvu, rozvíjať a modernizovať tieto služby, organizáciu práce a vlastné podporné činnosti. Nevyhnutnou súčasťou je však aj skvalitňovanie pracovného prostredia, bezpečnosti práce, rozvoj personálu a ochrana životného prostredia.

Vedenie obce Bacúch a ďalší vedúci zamestnanci majú záujem používať moderné technológie, a tak skvalitňovať poskytované služby a svoju vlastnú prácu. Neoddeliteľnou súčasťou týchto primárnych cieľov a zámerov je udržiavať a rozvíjať dobré vzťahy so všetkými partnermi, udržiavať dobré meno a povesť obce Bacúch v blízkom i širokom okolí. Vedenie obce Bacúch bude tieto ciele dosahovať výlučne prostriedkami a postupmi, ktoré sú plne v súlade so zákonmi SR a ostatnými zákonnými normami.

Možnosti spracúvania a prenosu údajov elektronickou cestou postupne zvyšujú ohrozenie zachovania diskrétnosti, súkromia a bezpečnosti. Istota, že bezpečnostný systém pracuje efektívne, spoľahlivo a za prijateľných nákladov, musí byť podložená overenými postupmi a metódami, ktoré boli použité pri jeho precíznom návrhu a realizácii. Na ochranu citlivých a osobných údajov sa v spolupráci s odborníkmi realizujú také organizačné, technické a technologické opatrenia, ktoré je možné ďalej rozvíjať a rozširovať dynamicky v závislosti na zmenách, a tým zachovávať stabilnú úroveň bezpečnosti.

Každý zamestnanec musí byť zaviazaný ochraňovať osobné údaje, citlivé údaje o obci Bacúch, osobné údaje občanov obce, osobné a obchodné údaje dodávateľov a partnerov pred prezradením, zničením, poškodením alebo stratou. Rovnako musí byť zaviazaný ochraňovať aj hmotné hodnoty obce Bacúch. Kvalitný a profesionálne navrhnutý program výchovy a vzdelávania zamestnancov má pomáhať zvyšovať zodpovednosť zamestnancov v otázkach bezpečnosti, zlepšovať ich odborné schopnosti v tejto oblasti a formovať ich bezpečnostné povedomie.

Obec Bacúch sa rozhodla primeranými prostriedkami chrániť svoje dobré meno a vysoký kredit a dôveru, ktorú má u svojich partnerov a u širokej verejnosti. Bezpečnosť jej aktív je jednou z prvoradých úloh a všetci zamestnanci si uvedomujú svoju individuálnu zodpovednosť pri jej zabezpečovaní.

Pri návrhu bezpečnostných opatrení, určených na ochranu kľúčových aktív a ich implementácii do existujúcich systémov a technologických reťazcov, budú uplatnené nasledovné zásady a ciele:

1. Zásada ochrany dôležitých systémov a komponentov informačného systému. Dôležité systémy a komponenty informačného systému sú tie časti, ktorých zlyhanie, zničenie alebo iný dôvod nedostupnosti by mal dopad na strategické záujmy. Cieľom je dosiahnuť minimalizáciu rizika zlyhania dôležitých súčastí informačného systému obce Bacúch, komunikačnej a bezpečnostnej infraštruktúry.
2. Zásada ochrany údajov v informačných systémoch. Údaje musia byť chránené vo všetkých formách – hlasovej, písomnej, elektronickej, počas ich spracovania a prenosu pomocou počítačov, faxov, telefónnej alebo počítačovej siete a počas ich archivácie. Cieľom je dosiahnuť ekonomicky primeranú a pritom spoľahlivú ochranu osobných a ekonomických údajov, údajov o obchodnej činnosti a o vlastnom know-how.
3. Zásady a ciele ochrany osôb a personálnej bezpečnosti. Obec Bacúch chce a musí chrániť práva osôb, ktorých údaje sú spracúvané. Zároveň budú podniknuté všetky opatrenia na ochranu informačného systému pred neautorizovanou činnosťou neoprávnených osôb alebo pred činnosťou oprávnených zamestnancov majúcich prístup ku chráneným údajom, ktorí by chceli tieto oprávnenia zneužiť alebo by mohli takto konať pod nátlakom. Obec Bacúch vytvorí predpoklady pre stabilizáciu kľúčových zamestnancov, najmä tých, ktorí sa podieľajú na rozvoji a prevádzke informačných technológií, ktoré podporujú jej strategické záujmy. Zároveň zabezpečí ochranu know-how, ktorý má a spravuje táto skupina zamestnancov.
4. Zásada ochrany hmotného majetku a finančných prostriedkov. Majetok obce Bacúch predstavuje značné hodnoty, preto je potrebné zabezpečiť, aby sa s týmito hodnotami nakladalo tak, aby nedošlo k ich poškodeniu, zničeniu alebo iným stratám.
5. Zásada ochrany dobrého mena. Náležitá pozornosť bude venovaná ochrane dobrého mena obce Bacúch. Cieľom je udržanie a skvalitňovanie svojho dobrého mena.
6. Zásada priradenia zodpovednosti za bezpečnosť. Ochrana aktív musí byť založená na princípe vlastníctva. Vlastníctvom sa v tomto prípade rozumie priradenie informácie, údaju, presne definovanej množiny údajov alebo iného aktíva zamestnancovi, ktorý sa k nim bude správať, akoby boli jeho osobným vlastníctvom, a teda bude mať osobný záujem na ich ochrane. Každý „vlastník“ musí mať definované práva a povinnosti, ktoré mu umožnia zabezpečiť spoľahlivú ochranu jemu „zverených“ údajov a aktív. Cieľom je presné vymedzenie práv a povinností zamestnancov, majúce za následok zvýšenie zodpovednosti a skvalitnenie kontroly.
7. Zásada hlásenia stavu bezpečnostného systému. Vedenie obce Bacúch a zamestnanci musia byť pripravení primerane reagovať na krízovú situáciu tak, aby sa minimalizovali jej následky. Činnosť bezpečnostného systému a užívateľov informačného systému bude

monitorovaná, bezpečnostné incidenty budú sledované a pravidelne vyhodnocované. Proti narušiteľom bezpečnostného systému budú zavedené primerané opatrenia v súlade s platnou legislatívou.

8. Zásada postupu implementácie bezpečnostného systému. Bezpečnostný systém musí byť implementovaný na základe rozpracovaných zásad tak, aby boli rešpektované možnosti a potreby obce Bacúch.

Bezpečnostné mechanizmy, ktoré sú alebo budú implementované v prostredí obce Bacúch na ochranu aktív, musia mať takú bezpečnostnú úroveň, aby vyhoveli požiadavkám legislatívy Slovenskej republiky, a to najmä v oblasti ochrany osobných údajov, ochrany duševného vlastníctva, noriem pre prevádzku a bezpečnosť informačných systémov, ochrany bezpečnosti pri práci, bezpečnosti osôb a majetku. Bezpečnostné mechanizmy musia zodpovedať platným slovenským technickým normám, štandardom a postupom z oblasti bezpečnosti. Tam, kde to je možné, budú aplikované bezpečnostné postupy v súlade s medzinárodnými normami ISO TR 27001 - 27005, ISO TR 13335, ISO TR 27000, BS 7799. Tam, kde to je možné, bude od technických riešení vyžadované dosiahnutie zhody s bezpečnostnou úrovňou podľa ITSEC E2. Reálny stav bezpečnostnej úrovne bude pravidelne sledovaný a vyhodnocovaný.

Táto kapitola Bezpečnostného projektu obce Bacúch je podkladom pre vypracovanie „Vyhlásenia“, ktoré nebude mať charakter dôverného dokumentu. „Vyhlásenie“ môže byť zverejnené na takých miestach a takou formou, aby bola zaistená informovanosť zamestnancov a širokej verejnosti o úsilí obce Bacúch ochraňovať osobné údaje a svoje aktíva.

2.3. Požiadavky na mechanizmy ochrany aktív

2.3.1. Ochrana systémov a komponentov IS

Systémy sa musia rozvíjať v súlade s najnovšími trendmi tak, aby bola zabezpečená spoľahlivosť, požadovaná výkonnosť a funkčnosť. V systémoch budú implementované také bezpečnostné mechanizmy, ktoré zabezpečia predovšetkým ich vysokú dostupnosť a integritu. Použité informačné technológie musia vyhovovať požiadavke kompatibility so zámermi rozvoja obce Bacúch a vzájomnej kompatibility medzi jednotlivými používanými systémami a systémami partnerov.

Operačné systémy

Prístup k službám jednotlivých systémov musí byť zabezpečený prostredníctvom bezpečného prihlásenia sa. Musí byť znemožnené neautorizované (nepovolené) zavedenie operačného systému z nepovoleného média a jeho používanie neautorizovanou osobou. Z bezpečnostného hľadiska je potrebné aplikovať také operačné a databázové systémy, ktoré spĺňajú požiadavky schválenej bezpečnostnej úrovne. Je potrebné minimalizovať rôznorodosť technologických platforiem operačných a databázových systémov.

Komunikačná infraštruktúra

Obec Bacúch má vybudovanú vlastnú počítačovú a komunikačnú infraštruktúru (počítačovú sieť), ktorá je primeraného rozsahu k jej potrebám.

Aj keď počítačová sieť obce Bacúch je pripojená k verejnej komunikačnej sieti (Internet) takými prostriedkami, ktoré znižujú riziko neoprávneného prístupu (útoku) z prostredia tejto verejnej siete, bude potrebné v prípade jej ďalšieho rozvoja aplikovať nové alebo preveriť existujúce oddelenie citlivých častí komunikačnej infraštruktúry. Kritické časti komunikačnej

infraštruktúry musia byť navrhnuté tak, aby umožnili vytvoriť záložné (redundantné) spojenia.

Vstupy do systému budú kontrolované na prítomnosť vírusov. Každý vstupný bod bude vybavený mechanizmom, ktorý bude robiť pravidelné prehliadky systému. Antivírusový systém bude pravidelne aktualizovaný s cieľom dosiahnuť vysokú odolnosť voči infiltráciám.

Komunikačné rozvody (počítačové siete, telekomunikačné siete) musia byť chránené pred poškodením, zničením a zneužitím. Pripojovanie zariadení ku komunikačnej infraštruktúre musí byť centrálne riadené a kontrolované, musí sa zamedziť pripojovaniu nepreverených systémov a systémov, ktoré neboli schválené príslušnými bezpečnostnými orgánmi obce Bacúch.

Archivácia a zálohovanie

Technológie zálohovania, archivácie a obnovy musia byť implementované tak, aby čas obnovy zodpovedal požiadavkám na zabezpečenie kontinuity funkcií. Musia byť navrhnuté a implementované procedúry, upravujúce zálohovanie údajov a programového vybavenia, v ktorých sa definuje najmä maximálne tolerovaná strata údajov – tzn. definuje maximálnu dobu medzi dvomi po sebe idúcimi zálohovacími procedúrami, a to pre každú jednu časť informačného systému.

Evidencia a správa porúch

V obci Bacúch musí byť navrhnutý a implementovaný primeraný systém podpory používateľov a systém správy porúch, ktorý zabezpečí detekciu, izolovanie, opravu a dokumentovanie chýb systémov a komponentov informačného systému.

2.3.2. Ochrana údajov

V obci Bacúch existuje niekoľko typov údajov, ktorých prezradenie, strata alebo zničenie by mali za následok negatívny dopad na fungovanie obce. Sú to najmä osobné údaje zamestnancov, obchodných partnerov a obyvateľov, údaje spracúvané ekonomickým a personálnym útvarom a údaje súvisiace s bezpečnosťou a ochranou.

Klasifikácia údajov

Požiadavky na ochranu pre všetky údaje nie sú rovnaké, preto bude potrebné stanoviť kategórie údajov podľa stupňa ich citlivosti a tiež kritériá zaraďovania údajov do jednotlivých kategórií. Pre každú kategóriu údajov sa určia také bezpečnostné mechanizmy, ktoré zaručia požadovanú dôvernosť, integritu a dostupnosť údajov počas celého ich celého životného cyklu.

Každý údaj, ktorý je spracúvaný, uložený alebo prenášaný prostredníctvom informačného systému, bude zaradený do jednej z kategórií citlivosti, ktorá určuje bezpečnostné požiadavky na jeho ochranu a pravidlá prístupu pre všetkých užívateľov. Klasifikáciou sa teda rozumie zaradenie údajov do jednej z kategórií citlivosti. Za klasifikáciu je zodpovedný vlastník údajov.

Aplikácia voliteľného riadenia prístupu k údajom

Prístup k údajom bude založený na princípe voliteľného riadenia. Každý vlastník v spolupráci s vedením obce určí pravidlá pre priradenie prístupových práv všetkým užívateľom oprávneným používať údaje v jeho správe. Aplikácia týchto pravidiel bude regulovaná príslušnými procedúrami a praktikami.

Aplikácia princípu mini-max

Každému zamestnancovi bude priradený minimálny rozsah prístupových práv, aký je možný na plnenie jeho pracovných úloh. Aplikovaním pravidla „mini-max“ je možné zaručiť prístup zamestnancov k údajom, ktoré sú potrebné pre výkon ich práce a zároveň zabezpečiť vysokú úroveň dôvernosti údajov.

Identifikácia a autentifikácia

Pri prístupe užívateľa k údajom sa bude vyžadovať identifikácia a autentifikácia. Každý používateľ pristupujúci k údajom musí mať jedinečné identifikačné údaje, na základe ktorých bude môcť získať oprávnenia pre prístup k údajom a funkciám systémov. Zdieľanie identifikačných údajov viacerými osobami nie je povoľované, bude sa monitorovať a vinníci budú postihnutí podľa platných predpisov. Rozdelenie kompetencií pri prístupe k zdrojom bude zároveň slúžiť aj k ochrane citlivých údajov, čím sa má zabrániť úniku údajov.

Definovanie zodpovednosti zamestnancov

Zamestnanci, ktorí prichádzajú alebo môžu prísť do styku s citlivými údajmi a informáciami počas výkonu svojej práce, musia byť zmluvne zaviazaní zachovávať mlčanlivosť o týchto údajoch a skutočnostiach. Súčasťou pracovnej zmluvy zamestnanca bude zoznam práv a povinností týkajúcich sa ochrany údajov vyplývajúcich z jeho pracovného zaradenia. Zamestnanci budú poučení o svojich právach a zodpovednostiach prostredníctvom výchovno-vzdelávacieho programu.

Monitorovanie prístupu k citlivým údajom

Prístup alebo pokus o prístup k citlivým údajom bude kontinuálne monitorovaný zodpovedajúcimi bezpečnostnými mechanizmami a vyhodnocovaný vedením obce. Neautorizované prístupy a pokusy o prístup, ktoré sú v rozpore s definovanými pravidlami, budú vyšetrené a proti narušiteľom budú zavedené opatrenia a postihy. V prípade výskytu takýchto narušení budú prijaté opatrenia na zvýšenie úrovne bezpečnosti.

Obmedzenie prístupu externých subjektov k citlivým údajom

Prístup zamestnancov externých subjektov k citlivým údajom bude obmedzený len na tie údaje, ktoré tieto subjekty potrebujú pre plnenie svojich povinností alebo záväzkov. Riadenie prístupu zamestnancov dodávateľov a partnerov bude upravené špecifickými procedúrami a technickými opatreniami.

Zamestnanci externých subjektov sa v areáloch, budovách a v priestoroch, kde sa nachádzajú citlivé údaje, budú môcť pohybovať len na základe odôvodnených potrieb. Všetky objekty a priestory budú rozdelené na viacero zón s rôznym režimom ochrany priestorov. Pre každú zónu bude vymedzený okruh oprávnených osôb, ktoré sa v danej zóne môžu samostatne pohybovať, budú stanovené pravidlá a procedúry pre prístup neoprávnených osôb do jednotlivých zón a spôsob zisťovania narušenia týchto zón. V zónach, v ktorých je to potrebné, budú zavedené špecifické procedúry identifikácie vstupujúcich osôb.

Zmluvy s dodávateľmi musia byť koncipované tak, aby zohľadňovali platnú slovenskú legislatívu v oblasti ochrany údajov, podmienky ochrany a bezpečnosti informačného systému stanovené riadiacimi dokumentmi. Rovnaké opatrenia sa týkajú aj systémov technickej a technologickej bezpečnosti.

Citlivé údaje nesmú bezdôvodne opustiť priestory Obecného úradu v Bacúchu. Ak je nevyhnutné, aby citlivé údaje opustili priestory Obecného úradu v Bacúchu, musia byť dodržané vnútorné predpisy a údaje musia byť vhodným spôsobom chránené pred zničením, modifikáciou alebo iným zneužitím. Citlivé údaje v IT zariadeniach, na médiách

a dokumentácia obsahujúca citlivé údaje musí byť pri vyradení z používania spoľahlivo zlikvidovaná.

Ochrana údajov prenášaných elektronicky

Elektronicky prenášané citlivé údaje budú chránené v súlade s požiadavkami na ochranu citlivých údajov v informačnom systéme. Musí byť stanovený presný a jasný režim, za akých podmienok je možné citlivé údaje v informačnom systéme a mimo neho prenášať.

2.3.3. Kvalitný a efektívny vývoj, ochrana autorských práv

Riadenie kvality procesu vývoja

Pri vývoji a rozvoji akejkoľvek časti informačného systému musí byť zabezpečená odbornosť a kvalita celého procesu vývoja a rozvoja. Pri vývoji sa budú uplatňovať formálne a správne metodické postupy a automatizované nástroje podporujúce efektívny vývoj, údržbu a prevádzkovanie aplikácií a systémov. Základnou požiadavkou na vývoj informačných systémov bude aj striktné oddelenie vývoja od produkčnej prevádzky. Budú unifikované platformy informačného systému tak, aby sa minimalizovali požiadavky na ľudské a finančné zdroje využívané pri vývoji a prevádzke.

Integrácia bezpečnostných požiadaviek

Pri vývoji a rozvoji informačného systému alebo systémov technickej ochrany budú v súlade s vnútornými predpismi obce Bacúch zohľadňované bezpečnostné požiadavky vlastníkov a požiadavky organizačných zložiek zodpovedných za bezpečnosť. Bezpečnostné požiadavky vyplývajúce z riadiacich dokumentov budú zakomponované do vyvíjaných častí informačného systému tak, aby sa eliminovali náklady na ich dodatočné zapracovanie po ukončení procesu vývoja. Na vývoji sa budú podieľať aj špecialisti zodpovední za bezpečnosť.

Bezpečnosť dokumentácie

Dokumentácia projektov informačného systému (t.j. zdrojové a vykonateľné kódy, implementačné postupy) alebo systémov technickej ochrany bude chránená pred prístupom neautorizovaných osôb a pred neautorizovanými zmenami.

Testovanie

Pred distribúciou nakúpeného alebo vyvíjaného programového vybavenia budú vykonané zodpovedajúce testy v testovacom prostredí tak, aby sa zamedzilo následným škodám v ostrej prevádzke. Rovnako aj systémy technickej ochrany budú podrobené zodpovedajúcim testom.

Ochrana autorských práv

Distribúcia softvéru bude riešená tak, aby nedochádzalo k nelegálnemu kopírovaniu softvéru. Cieľom pravidelných kontrol je odhaliť nelegálne používanie softvéru, z ktorého budú vyvodené sankcie voči osobám, ktoré konali úmyselne alebo nedbalo v súlade s platnou legislatívou.

2.3.4. Ochrana osôb a personálna bezpečnosť

Jedným z kľúčových aktív obce sú osoby. Osobami sa myslia najmä zamestnanci vykonávajúci činnosti priamo súvisiace s predmetom služieb obyvateľstvu, riadiaci zamestnanci a zamestnanci obslužných prevádzok, vrátane zamestnancov dodávateľov obce Bacúch, ktorí sa nachádzajú v jej priestoroch a s jej súhlasom. Osobám, ako jednému

z hlavných aktív, bude preto venovaná osobitná pozornosť s cieľom zabezpečiť vysoký štandard ochrany ich životov a zdravia.

Všetky systémy obce Bacúch budú primerane chránené pred nelegálnou alebo neautorizovanou činnosťou osôb.

V každej organizácii existujú vysoké hrozby zo strany vlastných zamestnancov, prípadne tretích osôb, ktoré sa môžu podieľať na útokoch na informačný systém alebo napomáhať pri realizovaní inej trestnej činnosti s cieľom získania finančného alebo obdobného prospechu. Ľudia sú najslabším článkom bezpečnostnej štruktúry, a preto obec Bacúch bude venovať tomuto problému zvýšenú pozornosť. V nasledujúcej časti sú stanovené základné zásady a bezpečnostné požiadavky, ktoré bude obec Bacúch aplikovať v oblasti personálnej bezpečnosti.

Zamedzenie neautorizovanému zhromažďovaniu a poskytovaniu údajov

IT zariadenia (počítače) obce Bacúch obsahujú osobné údaje zamestnancov, údaje o dodávateľoch, ekonomicko-finančné údaje ako aj ďalšie citlivé údaje o obyvateľoch. Pre obec Bacúch je neprijateľná strata dôvernosti, neautorizované sprístupnenie a zneužitie údajov a znalostí. Činnosť zamestnancov, neautorizované akcie a pokusy o narušenie bezpečnostného systému budú monitorované a vyhodnocované. V prípade, že sa zistí narušenie bezpečnosti, bude vykonané vyšetrovanie s cieľom objasniť príčiny, pôvod incidentu, eliminovať jeho následky a vyvodiť dôsledky.

Reakcia obce Bacúch pri nátlaku na zamestnancov

Jedným z hlavných zámerov obce Bacúch je, aby jej zamestnanci mali istotu, že podnikne všetky legálne kroky v prípadoch, keď budú vystavení tlaku nútenej nelegálnej spolupráce alebo vydierania. Vedenie obce Bacúch vyvinie maximálne úsilie s cieľom mať prehľad o počte a dôležitosti prípadov vydierania, ktorým môžu čeliť zamestnanci na jednotlivých pracoviskách. Vedenie obce Bacúch preberá zodpovednosť za účinnú a citlivú reakciu na tieto incidenty, pričom bude využitý systém hlásenia bezpečnostných incidentov.

Zníženie pravdepodobnosti omylu zamestnanca

Problémom, ktorý vyplýva z prístupu osôb k údajom a informáciám, je riziko náhodného omylu. Na ochranu pred týmto rizikom budú navrhnuté a uplatňované bezpečnostné a kontrolné mechanizmy a organizačné opatrenia, ktoré obmedzia pravdepodobnosť vzniku omylu a zabezpečia odhalenie každého omylu, ktorý môže spôsobiť hoci aj malé škody. Tieto opatrenia budú navrhované a testované v štádiu vývoja a testovania informačných systémov alebo systémov technickej bezpečnosti. Kontrolné mechanizmy budú zavedené do všetkých činností tak, aby sa zabránilo možnému narušeniu alebo podvodu predovšetkým zo strany zamestnancov, ale aj zo strany iných osôb.

Výchovno-vzdelávací program, bezpečnostné povedomie

Zodpovednosť a bezpečnostné povedomie zamestnancov obce Bacúch sa bude zvyšovať primeraným komplexom výchovno-vzdelávacích aktivít. Zamestnanci musia mať pocit zodpovednosti za ochranu hmotných aj nehmotných aktív obce Bacúch. Cieľom výchovno-vzdelávacieho programu je stotožnenie sa zamestnancov s realizovanými bezpečnostnými opatreniami a vytvorenie bezpečnostného povedomia. Cieľom výchovno-vzdelávacích aktivít bude zníženie rizík vyplývajúcich predovšetkým z činnosti zamestnancov a rozvíjanie prirodzenej lojality zamestnancov k obci Bacúch.

Stanovenie zodpovednosti a právomoci zamestnancov

Každému zamestnancovi budú priradené také zodpovednosti a právomoci, aby mohol vykonávať úlohy, ktoré mu vyplývajú z jeho pracovnej náplne. Oprávnenia fyzického prístupu do budov a ich častí, kde sa nachádzajú chránené aktíva obce Bacúch, budú pre každého zamestnanca jasne a presne stanovené s ohľadom na jeho zodpovednosti a právomoci. Každý zamestnanec bude mať stanovený rozsah prístupu k zdrojom informačného systému.

Poučenie zamestnancov o ich zodpovednostiach a právomociach v rámci organizačnej štruktúry bezpečnosti sa bude vykonávať v rámci výchovno-vzdelávacích aktivít. Každý zamestnanec bude ručiť za dôvernosť svojich autentizačných prostriedkov a identifikačných údajov, ktoré mu majú umožniť vstup do kontrolovaných častí objektov resp. do informačného systému. Každý zamestnanec, ktorý poruší povinnosti, bude postihnutý sankciami definovanými v interných predpisoch obce Bacúch, prípadne v legislatíve SR. Informovanosť o postihoch za porušenie bezpečnostných pravidiel sa dosiahne prostredníctvom výchovno-vzdelávacieho programu.

Aplikácia pravidla čistého stola

Zamestnanci, a najmä riadiaci pracovníci, musia dodržiavať tzv. „pravidlo čistého stola“. Všetky dokumenty, materiály, elektronické nosiče údajov, autentizačné prostriedky a pod. sa budú na stole nachádzať len v čase, ktorý je potrebný na prácu s nimi. Po ukončení práce sa tieto materiály presunú na určené bezpečné miesto.

Všetky nepotrebné údaje a elektronické a papierové nosiče týchto údajov sa znehodnotia spôsobom, ktorý bude stanovený vnútornými predpismi obce Bacúch.

Preverenie osôb s prístupom k citlivým údajom

Pre proces prijímania nových zamestnancov, ktorí môžu prísť do styku s citlivými údajmi, budú aplikované také pravidlá a postupy, ktoré vylúčia možnosť prijatia nespoľahlivých osôb a osôb s kriminálnou minulosťou. Tieto pravidlá a postupy budú použité aj pre preverenie zamestnancov dodávateľov, ktorí môžu prísť do styku s citlivými údajmi alebo dôležitými komponentmi informačného systému. Pri skončení pracovného pomeru každého zamestnanca bude tento poučený o povinnosti zachovať dôvernosti citlivých údajov.

Motivovanie zamestnancov

Dôležitým prvkom bezpečnostného systému je stabilizácia pracovného kolektívu, predovšetkým kľúčových zamestnancov. Bude použitý vhodný systém motivovania a odmeňovania kľúčových zamestnancov, ktorých odchod môže vážne ohroziť funkčnosť informačných a bezpečnostných systémov.

Pravidlá pre výber a prácu dodávateľov

Pri výbere dodávateľov budú zároveň s kritériami kvality brané do úvahy aj bezpečnostné požiadavky obce Bacúch. Produkty a služby, ktoré budú predmetom dodávky musia vyhovovať bezpečnostným požiadavkám obce Bacúch.

2.3.5. Technická bezpečnosť objektov a priestorov

Ochrana budov, areálov a hmotného majetku obce Bacúch je dôležitým bezpečnostným prvkom ochrany osôb, údajov a zabezpečenia všetkých funkcií obce Bacúch. Cieľom ochrany priestorov je umožniť dosiahnutie požiadaviek, ktoré sú kladené na ochranu osôb v priestoroch Obecného úradu v Bacúchu a na ochranu údajov bez ohľadu na ich citlivosť a požadovanú ochranu. Bezpečnostné mechanizmy majú zabezpečiť ochranu priestorov

pred neoprávneným vniknutím do nich a ochranu hmotného majetku pred stratou, zničením a krádežou.

Ochrana fyzického prístupu ku kritickým komponentom informačného systému a ostatným dôležitým aktívam

Prístup k dôležitým komponentom informačného systému alebo ostatným dôležitým aktívam bude riadený vhodnými technickými prostriedkami. Riadenie prístupových práv bude upravovať praktiky a procedúry vypracované počas implementácie návrhov opatrení a modifikované podľa miestnych podmienok.

Pracovný priestor, v ktorom sa nachádzajú komponenty informačného systému alebo ostatné dôležité aktíva, bude v neprítomnosti zamestnancov chránený vhodnými bezpečnostnými mechanizmami, ktoré budú vybrané v závislosti od druhu komponentu a spôsobu umiestnenia.

Používanie, uchovávanie a správu kľúčov alebo iných prostriedkov, ktoré umožňujú vstup do chránených priestorov, budú upravovať postupy vypracované počas implementácie návrhov opatrení a modifikované podľa miestnych podmienok. Tieto musia upravovať aj spôsob prístupu mimo pracovných hodín pre prípad havárie alebo práce mimo bežnej pracovnej doby.

Budovanie vhodných priestorov

Komponenty IS alebo iné dôležité aktíva, ktoré to vyžadujú, sa budú nachádzať v priestoroch, ktoré spĺňajú špeciálne požiadavky na ich technickú a režimovú bezpečnosť. Pri projektovaní výstavby alebo rekonštrukcie priestorov alebo objektov musia byť akceptované odborné požiadavky zamestnancov zodpovedných za bezpečnosť a ochranu aktív.

2.3.6. Ochrana dobrého mena a nehmotné aktíva

Nehmotné aktíva, ktoré musí obec Bacúch chrániť sú predovšetkým jej dobré meno, kredit u obyvateľov a ďalších partnerských organizácií a etický štandard zamestnancov. Nehmotné aktíva sú neoddeliteľnou a veľmi dôležitou súčasťou vlastníctva obce Bacúch, zvlášť v období, kedy sa prirodzené konkurenčné prostredie rozširuje aj za hranice SR.

Pre oblasť ochrany aktív budú prijaté také technické a organizačné opatrenia, ktoré majú vplyv aj na ochranu týchto nehmotných aktív.

Budú vypracované také procedúry, ktoré znemožnia alebo sťažia konanie zamestnancov a iných osôb, ktoré by mohli poškodiť dobré meno obce Bacúch.

2.3.7. Poznávanie stavu bezpečnostného systému a hlásenie bezpečnostných incidentov

Významným faktorom efektívneho bezpečnostného systému je jeho schopnosť poskytnúť informácie o aktuálnom stave bezpečnostných opatrení implementovaných na ochranu aktív.

Stav bezpečnostného systému bude monitorovaný využitím automatizovaných prostriedkov s centrálnou správou. Monitorovanie stavu bezpečnostného systému musí byť zamerané na sledovanie neautorizovaných činností užívateľov, odhaľovanie prienikov do informačného systému alebo do chránených zón a predikciu bezpečnostných incidentov.

Monitorovací systém nesmie byť zneužitý na sledovanie zamestnancov. V prípade, že sa zistí narušenie bezpečnosti, bude vykonané vyšetrovanie s cieľom objasniť príčiny, pôvod incidentu, eliminovať jeho následky a vyvodiť dôsledky.

Bezpečnostné incidenty, ktoré nie je možné monitorovať automatizovanými prostriedkami, budú monitorované doterajšími zaužívanými metódami. Rovnako aj riešenie takýchto incidentov bude prebiehať zavedenými metódami vlastného vyšetrovania, pokiaľ to

situácia dovoľuje. Všetky takto zistené bezpečnostné incidenty budú zaznamenané a budú pravidelne vyhodnocované.

Bezpečnostný incident je akákoľvek udalosť, ktorej cieľom je narušiť bezpečnosť informačného systému, technickú bezpečnosť priestoru alebo objektu, bezpečnostný mechanizmus aplikovaný v rámci prevádzkovaných technológií. Bezpečnostný incident môže byť vyvolaný náhodným faktorom, neúmyselným činom alebo úmyselným útokom, alebo podvodom.

Bezpečnostný incident je povinný hlásiť každý zamestnanec svojmu nadriadenému. Zamestnanci budú poučení o tom, čo sa považuje za bezpečnostný incident, budú s nimi prebraté typové prípady incidentov a detailne prebratý spôsob, ako majú incident ohlásiť, aby nedošlo k zmareniu jeho vyšetrenia.

Každý bezpečnostný incident bude zaradený do jednej z kategórií, podľa naliehavosti jeho riešenia:

- okamžitý zásah – incidenty, ktoré pravdepodobne spôsobia škody alebo ich už spôsobili, ohrozujú chod, životy a zdravie osôb, ohrozujú bezpečnosť alebo plynulosť spracovania údajov v informačnom systéme, prípadne sa môžu rozšíriť (požiar, nedostupnosť zdrojov, komunikácií a pod.),
- prioritný zásah – incidenty, ktoré svojou podstatou porušili platnú legislatívu SR alebo interné normy obce Bacúch a následne môžu spôsobiť narušenie bezpečnosti (neštandardné akcie dodávateľa, porušenie autorských práv, podozrenie zo zneužívania údajov a pod.),
- rutinný zásah – incidenty, ktoré sú očakávané alebo existuje podozrenie z ich výskytu (vírusy, opakované zablokovanie a pod.).

2.3.8. Aktíva obce Bacúch

Jedným z predpokladov dobre spracovanej rizikovej analýzy je vymedzenie aktív obce Bacúch, ktoré majú priamy vzťah k ochrane a bezpečnosti. Aktíva sú zaradené do nasledujúcich kategórií:

1. Počítače, programové vybavenie, operačné systémy – do tejto kategórie patrí výpočtová technika, ktorá spracúva vstupy používateľov, ukladá údaje a poskytuje výstupy bez ohľadu na formy.
2. Komunikačná infraštruktúra – sú to všetky prvky komunikačnej infraštruktúry od rozvodov počítačovej siete a až po opakovače (HUB-y), prepínače (switch-e) a smerovače (routre).
3. Údaje, informácie – sú to všetky spracúvané a ukladané údaje a informácie bez ohľadu na ich formu a nosič, na ktorom sú uložené.
4. Personál, zamestnanci a osoby.
5. Prostredie, budovy a ich zariadenia.
6. Obec Bacúch a riadenie – okrem organizačnej štruktúry sú to aj postupy riadenia, kontrolné mechanizmy.
7. Podporná infraštruktúra – do tejto kategórie patria všetky činnosti, ktoré aj keď bezprostredne nesúvisia s predmetom činnosti obce Bacúch, sú pre jej činnosť nevyhnutné (tepelné hospodárstvo, dopravné a komunikačné služby a pod.).
8. Ostatné.

Obec Bacúch za kľúčové považuje najmä informácie o svojich zamestnancoch, občanoch, dodávateľoch a obchodných partneroch, o používaných postupoch, spôsobe riadenia obce ako aj o svojich plánoch a zámeroch do budúcnosti. Prirodzenou snahou obce Bacúch je dodržiavať platnú slovenskú legislatívu. Aktíva sú detailne identifikované v rizikovej analýze.

2.3.9. Vymedzenie okolia

Pre kvalitný návrh Bezpečnostnej politiky je nevyhnutné dobré poznanie okolia, ktoré vplýva na obec Bacúch. Okolie je možné rozčleniť do nasledujúcich kategórií:

- fyzické vplyvy – sú to najmä vplyvy životného prostredia, riziká priemyselných havárií a prírodných vplyvov prípadne katastrof. Obec Bacúch pôsobí vo viacerých lokalitách - v budovách.
- vplyvy fyzických osôb nezamestnaných na Obecnom úrade v Bacúchu a jeho inštitúciách – všetky osoby nezamestnané na Obecnom úrade v Bacúchu predstavujú potenciálne hrozby. Špeciálnu skupinu predstavujú bývalí zamestnanci, s ktorými bol rozviazaný pracovný pomer z rozhodnutia obce Bacúch (typicky pre neplnenie pracovných povinností a porušovanie pracovnej disciplíny), a teda by mohli mať osobný záujem na poškodení obce Bacúch.
- vplyvy fyzických osôb zamestnaných na obecnom úrade a pod neho spadajúcich organizácií – vlastní zamestnanci vždy predstavujú významný rizikový faktor, pretože vzájomná a prirodzená lojalita vo vzťahu zamestnanec - zamestnávateľ oslabuje možnosť včasnej indikácie hrozieb a rizík. Aj keď sa počíta s lojalitou, budú tieto potenciálne hrozby primerane zohľadnené v rizikovej analýze.
- vplyvy iných právnických osôb – v súčasnosti nie sú vedeniu obce Bacúch známe hrozby zo strany iných právnických osôb, avšak ani tieto hrozby nie je možné vylúčiť.

2.3.10. Vymedzenie okruhu zvyškových rizík

Riziká identifikované v analýze bezpečnosti sa bude obec snažiť pokryť takými opatreniami, ktoré minimalizujú úroveň rizika, a teda minimalizujú ohrozenie obce. Obec sa rozhodla, že vo všeobecnosti je možné ponechať opatreniami nepokryté tie riziká, ak:

- na minimalizáciu rizika je potrebné prijať nových zamestnancov,
- na minimalizáciu rizika je potrebné vynaložiť investíciu vo výške 1000 €, celkovo však nie viac ako 3000 €,
- na prevádzku opatrení na minimalizáciu rizika bude potrebné ročne vynaložiť viac ako 1000 €,
- na minimalizáciu rizika je potrebné zásadne zmeniť vnútornú organizačnú štruktúru.

Opatrenia, ktoré zostanú v okruhu zvyškových rizík budú pravidelne posudzované a prehodnocované v kontexte aktuálnej kondície obce a jej ekonomických a personálnych možností.

2.3.11. Implementácia Bezpečnostnej politiky

Nevyhnutnou podmienkou spoľahlivej a efektívnej práce celého bezpečnostného systému je splnenie základných požiadaviek na implementáciu bezpečnostných mechanizmov, vypracovanie procedúr a zavedenie organizačnej štruktúry bezpečnosti v podmienkach obce Bacúch. Tieto požiadavky sú definované v Bezpečnostnej politike a mali by byť ďalej rozpracované v interných predpisoch a metodických pokynoch.

Bezpečnostná politika je dokument, ktorý schvaľuje vedenie a určuje:

- hlavné ciele, ktoré sa majú dosiahnuť implementáciou bezpečnostnej politiky,
- postup implementácie jednotlivých súčastí bezpečnostného systému a zodpovednosť zamestnancov za túto implementáciu,
- zodpovednosť za prevádzku a kontrolu bezpečnostného systému a popisuje vzťahy medzi organizačnými zložkami vo veciach bezpečnosti,
- sankcie za porušenie smerníc, bezpečnostných opatrení a za neplnenie a zanedbanie povinností,
- dobu a spôsob aktualizácie kľúčových dokumentov dotýkajúcich sa bezpečnosti (najmä Bezpečnostného projektu),
- spôsob a periodicitu vyhodnocovania stavu bezpečnosti,
- postup pri povoľovaní použitia nových komponentov informačného systému a zariadení majúcich vplyv na bezpečnosť a ochranu.

Zmeny existujúcich komponentov, nové projekty a zavádzanie nových technológií sa bude uskutočňovať za spoluúčasti zamestnancov zodpovedných za bezpečnosť s cieľom zabezpečiť strategické ciele na ochranu jednotlivých aktív definovaných v tomto dokumente.

Informačné technológie už v súčasnosti majú dôležité postavenie a ich význam bude postupne rásť. Ich správna funkcia a využitie sa stanú základným predpokladom skvalitňovania poskytovaných služieb. Elektronické spracovanie údajov so sebou prináša zvýšené nároky na informačný systém a ochranu údajov pred zneužitím, poškodením a stratou. Ochrana a bezpečnosť je chápaná vedením obce Bacúch ako nepretržitý proces. Z tohto pohľadu sa bude kontinuálne posudzovať úroveň bezpečnosti a sústavne reagovať na nový vývoj, zmeny a zistené nedostatky.

2.3.12. Vedenie dokumentácie

Predpokladom kvalitného riadenia a kontrolovania každej organizovanej činnosti, vrátane implementácie Bezpečnostnej politiky, je konzistentná a jasná dokumentácia. Obec Bacúch má zámer vypracovať všetky dokumenty nevyhnutné pre riadenie bezpečnosti a pre efektívnu kontrolu prijatých opatrení.

Súčasťou tejto dokumentácie bude najmenej:

- vyhlásenie o zaručení dostatočnej bezpečnosti, ktoré je verejným dokumentom a je určený širokej verejnosti,
- tento Bezpečnostný projekt a Bezpečnostná politika,
- krízový plán – plán zvládnutia krízových situácií alebo implementácia opatrení súvisiacich s bezpečnosťou informačných systémov a údajov do existujúceho krízového plánu,
- plány obnovy a zotavenia, ktoré určujú postupy a procedúry, ako sa bude postupovať pri obnove narušených funkcií,
- bezpečnostné smernice a predpisy pre prevádzku informačného systému,
- záznamy o prevádzke informačných systémov, bezpečnostných systémov, vrátane záznamov o vyhodnotení incidentov,
- záznamy o vykonaných školenia a poučeniach, vrátane prezenčných listín a popisu obsahu školení a poučení.
-

Pre každý dokument musia byť definované a známe tieto vlastnosti:

- autor (autori) dokumentu a meno pracovníka, ktorý dokument schválil,
- dátum poslednej revízie a v prípade obmedzenej platnosti aj dátum, do kedy dokument platí,
- evidenčné znaky – všetky dokumenty budú centrálne evidované,
- archivačné znaky - najmä údaj o tom, kedy a za akých podmienok je možné dokument skartovať,
- rozsah osôb resp. organizačných zložiek, pre ktoré je dokument záväzný,
- zmenové listy alebo iný vhodný spôsob zmien dokumentov.

2.3.13. Postup implementácie Bezpečnostnej politiky

Zavedenie Bezpečnostnej politiky do života obce Bacúch

Bezpečnostná politika a ďalšie bezpečnostné dokumenty budú považované za riadiace dokumenty bezpečnosti. Ich autorizácia vedením podmieňuje začiatok implementácie bezpečnostných mechanizmov. Krok autorizácie je dôležitým aktom, ktorý schváli rozsah, finančnú, personálnu a časovú náročnosť projektu komplexného riešenia ochrany a bezpečnosti informačného systému ako aj ostatných oblastí vnútornej bezpečnosti. Implementácia bude rozčlenená do etáp tak, aby v optimálnej miere boli prispôsobené možnostiam a potrebám obce Bacúch a aby boli dosiahnuté strategické ciele Bezpečnostnej politiky. Pri implementácii sa bude postupovať takto:

- Spracovanie detailnej analýzy rizík pre vybrané aktíva z oblasti informačných systémov, oblasti technológií, fyzickej a režimovej ochrany, ochrany osôb.
- Vypracovanie bezpečnostných dokumentov.
- Okamžité kroky ochrany – realizácia krátkodobých opatrení na odstránenie najväčších rizík.
- Zavedenie, resp. skvalitnenie identifikačného systému a riadenia prístupu k zdrojom informačného systému.
- Zabezpečenie bezpečnosti interných a externých prenosových kanálov (LAN, Internet, telefón, GSM, fax).
- Integrácia bezpečnostných mechanizmov do aplikácií informačného systému.
- Zvýšenie technickej ochrany hmotných aktív, najmä rozčlenenie do zón, stanovenie a zabezpečenie režimu pre tieto zóny.
- Realizácia opatrení technickej a režimovej ochrany pre ochranu zamestnancov a im zverených prostriedkov.
- Návrh a implementácia bezpečnostných mechanizmov do bežnej prevádzky a chodu obce Bacúch (automatizovaných aj neautomatizovaných).
- Sledovanie a vyhodnocovanie stavu bezpečnosti informačného systému.
- Realizácia systémových a organizačných opatrení, realizácia výchovno-vzdelávacieho programu.
- Zavedenie auditu.

Zavedenie bezpečnostných mechanizmov a opatrení je dlhodobý projekt, ktorý musí reflektovať na všetky technologické, kapacitné, personálne a finančné požiadavky a možnosti obce Bacúch. Preto uvedená postupnosť môže byť zmenená tak, aby spĺňala uvedené požiadavky a možnosti.

Udržiavanie Bezpečnostnej politiky po ukončení zavedenia

Ukončením zavedenia nedochádza k trvalému vyriešeniu bezpečnosti informačného systému, k trvalému vyriešeniu technickej a režimovej ochrany majetku a ochrany osôb. Nevyhnutnou podmienkou spoľahlivej a efektívnej práce celého bezpečnostného systému je neustále vyhodnocovanie jeho používania, vyhodnocovanie incidentov, aktualizácia dokumentov a kritické prehodnocovanie schopností bezpečnostného systému plniť svoje funkcie.

Informačné technológie považuje obec Bacúch za kľúčové technológie a údaje za kľúčové aktívum, a preto prehodnocovanie a aktualizáciu bezpečnostných dokumentov považuje za nepretržitý proces, a preto prijme také opatrenia, aby ochrana a bezpečnosť všetkých svojich aktív bola trvalo zachovaná.